

USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

Publication number: JP2002514802 (T)

Publication date: 2002-05-21

Inventor(s):

Applicant(s):

Classification:

- international: **G06F13/00; G06F15/00; H04L12/56; H04L12/58; H04L12/66; H04L29/06; G06F13/00; G06F15/00; H04L12/56; H04L12/58; H04L12/66; H04L29/06; (IPC1-7): G06F13/00; G06F15/00; H04L12/66**

- European: **H04L29/06; H04L29/06S2B; H04L29/06S2B6; H04L29/06S4B1; H04L29/06S8**

Application number: JP20000547748T 19990429

Priority number(s): US19980084014P 19980504; US19990295966 19990421; WO1999US09362 19990429

Also published as:

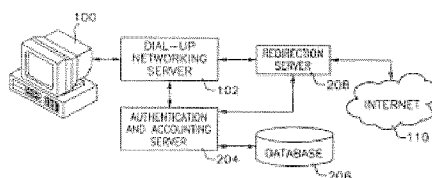
JP3588323 (B2)
WO9957866 (A1)
US2005021943 (A1)
US6779118 (B1)
HK1036707 (A1)

more >>

Abstract not available for JP 2002514802 (T)

Abstract of corresponding document: **WO 9957866 (A1)**

A data redirection system for redirecting user's data based on a stored rule set. The redirection of data is performed by a redirection server, which receives the redirection rules sets for each user from an authentication and accounting server, and a database. Prior to using the system, users authenticate with the authentication and accounting server, and receive a network address. The authentication and accounting server retrieves the proper rule set for the user, and communicates the rule set and the user's address to the redirection server. The redirection server then implements the redirection rule set for the user's address. Rule sets are removed from the redirection server either when the user disconnects, or based on some predetermined event. New rule sets are added to the redirection server either when a user connects, or based on some predetermined event.



Data supplied from the **espacenet** database — Worldwide

CLAIMS

(57)[Claim(s)]

[Claim 1]

A database including an item which makes each of two or more user ID correlate with a rule set only for [each] a user,
A dial up network server which receives user ID from a user's computer,
A redirection server connected to a network of said dial up network server and the public,
It is an automatic data redirection system only for a user containing attestation and a fee collection server which are connected to said database, said dial up network server, and said redirection server,
Said dial up network server transmits a temporary assignment network address for the 1st user ID to one of the computers of said user, and said 1st user ID to said attestation and a fee collection server,
Said attestation and a fee collection server access said database, and a rule set and said temporary assignment network address only for said each user who correlates with said 1st user ID are transmitted to said redirection server, An automatic data redirection system only for a user, wherein data turned to said public's network is processed by said redirection server according to a rule set only for [said each] a user from one of the computers of said user.

[Claim 2]

The system according to claim 1 by which said redirection server performs further control to two or more data which frequents said user's computer according to a rule set only for [said each] a user.

[Claim 3]

The system according to claim 1 by which said redirection server prevents further data which frequents said user's computer according to a rule set only for [said each] a user.

[Claim 4]

The system according to claim 1 by which said redirection server permits further data which frequents said user's computer according to a rule set only for [said each] a user.

[Claim 5]

The system according to claim 1 by which said redirection server redirects further data which frequents said user's computer according to a rule set only for [said each] a user.

[Claim 6]

The system according to claim 1 by which said redirection server redirects data from said user's computer to two or more addresses further according to a rule set only for [said each] a user.

[Claim 7]

The system according to claim 1 which said database item about said two or more user ID is made to correlate with a common rule set only for [each] a user.

[Claim 8]

A database including an item which makes each of two or more user ID correlate with a rule set only for [each] a user,
A dial up network server which receives user ID from a user's computer, A redirection server connected to a network of said dial up network server and the public, In a system containing attestation and a fee collection server which are connected to said database, said dial up network server, and said redirection server,
A stage of transmitting a temporary assignment network address for the 1st user ID to one of the computers of said user, and said 1st user ID to said attestation and a fee collection server from said dial up network server,
A rule set only for [said each] a user correlated with said 1st user ID, Said temporary assignment network address is transmitted to said redirection server from said attestation and a fee collection server, How to perform automatic data redirection only for a user including a stage of processing data turned to said public's network, from one of the computers of said user according to a rule set only for [said each] a user.

[Claim 9]

A method according to claim 8 of including further a stage which controls two or more data which frequents said user's computer according to a rule set only for [said each] a user.

[Claim 10]

A method according to claim 8 of including further a stage which prevents data which frequents said user's computer according to a rule set only for [said each] a user.

[Claim 11]

A method according to claim 8 of including further a stage of permitting data which frequents said user's computer according to a rule set only for [said each] a user.

[Claim 12]

A method according to claim 8 of including further a stage which redirects data which frequents said user's computer

according to a rule set only for [said each] a user.

[Claim 13]

A method according to claim 8 of including further a stage which redirects data from said user's computer to two or more addresses according to a rule set only for [said each] a user.

[Claim 14]

A method according to claim 8 which you are made to correlate with a rule set only for [each] a user in which said two or more user ID is still more common, including further a stage which generates a database item about said two or more user ID.

[Claim 15]

It is an automatic data redirection system only for a user containing a redirection server currently programmed using a user's rule set correlated with a temporary assignment network address,

At least one function in two or more functions used in order that said rule set may control data exchanged between said user and a public network is included,

An automatic data redirection system only for a user, wherein said redirection server is constituted so that change of at least some said rule sets correlated with said temporary assignment network address may be enabled.

[Claim 16]

The system according to claim 15 constituted so that said redirection server may enable change of at least some said rule sets according to time.

[Claim 17]

The system according to claim 15 constituted according to data which said redirection server is transmitted to a user, or is transmitted by user so that change of at least some said rule sets may be enabled.

[Claim 18]

The system according to claim 15 constituted so that said redirection server may enable change of at least some said rule sets according to one or more locations which a user accesses.

[Claim 19]

Data transmitted by data in which said redirection server is transmitted to time and a user, or user, Or the system according to claim 15 constituted according to a certain combination of one or more locations which a user accesses so that change of at least some said rule sets may be enabled.

[Claim 20]

The system according to claim 15 constituted so that it may make it possible for said redirection server to respond to time, and to delete or restore said at least a part of rule.

[Claim 21]

The system according to claim 15 constituted so that said redirection server may enable deletion or restoration of at least some said rule sets according to data transmitted by data transmitted to a user, or user.

[Claim 22]

The system according to claim 15 constituted so that said redirection server may enable deletion or restoration of at least a part of said rule according to one or more locations which a user accesses.

[Claim 23]

Data transmitted by data in which said redirection server is transmitted to time and a user, or user, Or the system according to claim 15 constituted according to a certain combination of one or more locations which a user accesses so that deletion or restoration of at least a part of said rule may be enabled.

[Claim 24]

The user side connected to a computer by which said redirection server uses said temporary assignment network address, The system according to claim 15 by which said computer which has the network side connected to a computer network, and uses said temporary assignment network address is connected to said computer network via said redirection server.

[Claim 25]

The system according to claim 24 by which a command to said redirection server for changing said rule set is received said user side of said redirection server by one or more by the side of said network of said redirection server.

[Claim 26]

A rule set of a user made to correlate with a temporary assignment network address including an included redirection server and said user's rule set, In a system including at least one function in two or more functions used in order to control data exchanged between said user and a public network,

While said user's rule set is freely made to correlate with said temporary assignment network address in said redirection server, How to perform data redirection only for a user including a stage of changing at least some said user's rule sets.

[Claim 27]

A method according to claim 26 of including further a stage of changing at least some said user's rule sets, or more according to one of data transmitted by data transmitted to time and a user, or user, and one or more of the locations which a user accesses.

[Claim 28]

A method according to claim 26 of including further a stage which responds or more to one of data transmitted by data transmitted to time and a user, or user, and one or more of the locations which a user accesses, and deletes or restores at least some said user's rule sets.

[Claim 29]

A method comprising according to claim 26:

The user side connected to a computer by which said redirection server uses said temporary assignment network address.

It has the network side connected to a computer network, Via said redirection server, said computer which uses said temporary assignment network address is connected to said computer network, and said method, A stage of receiving a command by said redirection server in order to change at least some said user's rule sets said user side of said redirection server or more by one by the side of said network of said redirection server.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

The field of invention

concerning the field of Internet communication in more detail, this invention relates to the database for using the traffic of the Internet for carrying out redirection (redirect) and filter (filter) dynamically.

[0002]

The background of invention

In the conventional system as shown in drawing 1, when the user of the Internet establishes connection with an Internet Service Provider (ISP), A user establishes a physical connection first between his own computer 100 and the dial up network server (called a dialing and a network server) 102, The dial up network server 102 is provided with its own user ID and password. A dial up network server sends user ID and a password to the next at attestation and the fee collection server 104 of ISP with a temporary Internet Protocol (IP) address for use by the user. Detailed explanation of IP communications protocol is indicated to "Internetworking with TCP/IP, 3rd ed., Douglas Comer, Prentice Hall, 1995."

These whole contents are included in this Description as a quotation.

When inspecting user ID and a password using the database 106, attestation and a fee collection server, In order to enable the user to use an IP address temporarily which is assigned to the user by the dial up network server, an authentication message is sent to the dial up network server 102, it assigns with connection the next, and an IP address is recorded. When a user requires from the Internet 110 during this session via the gateway 108, this end user will be identified by a temporary assignment IP address always.

[0003]

Redirection of INTERNET traffic is performed about World-Wide-Web (WWW) traffic (traffic which will use HTTP (HyperText Transfer Protocol) if it states still more clearly) in most cases. However, redirection is not limited to WWW traffic but this idea is effective in all the IP services. a demand of the user who asks for a WWW page (typically html (HyperText Markup Language) file) in order to show how redirection is performed -- being certain -- others -- the following example redirected to a WWW page will be considered. First, a user is a WWW browser (typically) by carrying out typing of the URL (universal resource locator), or clicking a URL link. It orders the software which operates on a user's PC to access the page on a remote WWW server. Please care about that URL provides the information about a communications protocol, the location (typically an Internet domain name or an IP address) of a server, and the location of the page concerned on a remote server. A browser sends a demand to a server and requires an applicable page of the next. Answering this user's demand, a web server sends the demanded page to a browser. However, a user's redirection starts, including [therefore] the html code ordered that this page requires other WWW pages of some kind of that browser. A browser requires the redirected WWW page of the next according to URL contained in the html code of the first page. Or redirection is able to be performed also by ordering to execute programs, such as a Java applet, to a browser, and coding a page so that this program may redirect a browser. One of

the faults of the present redirection technology is a remote side, i.e., the WWW server side, I hear that control of redirection is not a local, i.e., user, side, and it has it. Namely, redirection is performed by the remote server and is not performed depending on a user's local gateway.

[0004]

It is possible by using a firewall device or other packet-filtering equipment in the past several years to filter the packet in an Internet Protocol (IP) layer. In order that filtering of a packet may carry out the filter of the packet which enters into a private network from the purpose of security, it is used in most cases, but when programmed properly, it is also possible to carry out the filter of the output packet sent to a specific address from a user. The type of IP service included in an IP packet is identified, and packet filtering can be filtered based on discernment of this. For example, the packet filter can judge whether a packet contains FTP (file transfer protocol) data, WWW data, or Telnet session data. This service identification is realized by identifying the terminal port number included in each IP packet header. The port number follows the standards of the industry, in order to realize compatibility between equipment. Packet-filtering equipment enables a network administrator to carry out the filter of the packet based on a source and/or destination information, and the type of the service transmitted within each IP packet. Unlike redirection technology, packet-filtering technology enables control by the side of the local of network connection, and enables control by a network administrator typically. However, since it is static, packet filtering is restricted dramatically. Once a packet-filtering rule is programmed by a firewall device or other packet-filtering equipment, the packet-filtering rule set up only by reprogramming such equipment manually cannot be changed.

[0005]

Packet-filtering equipment is used with a proxy server system in many cases, and in order that this proxy server system may realize control of access to the Internet and may control access to WWW, it is used in most cases. In typical composition, a firewall device or other packet-filtering equipment carry out the filter of all the WWW demands from the local network to the Internet except for the packet from a proxy server. That is, a packet filter or a firewall prevents all the traffic sent out of the local network connected to the remote server on the port 80 (standard WWW port number). However, such traffic by which this packet filter or firewall is sent and received to the proxy server (proxy server) approves. Typically, the proxy server is programmed with 1 set of addresses which must be prevented, and the packet to which it was forced to the prevented address is not transmitted. When a proxy server receives a packet, in order to acquire recognition, an address is inspected in contrast with a database. If the address is approved, a proxy server will only transmit the packet between a local user and the remote server of the outside of a firewall. However, the proxy server is limited to preventing or permitting access of the specific system terminal to a remote database.

[0006]

The latest system is indicated by US,5,696,898,B. The database (.) which this patent does not control [an open data base or (when that is not right)] with a specific specific IP address inside a firewall That is, the system similar to a proxy server which enables a network administrator to restrict accessing the information from WWW/Internet is indicated. According to this disclosure, this system has a relational database which enables a network administrator to restrict that a specific terminal or terminal group accesses a specific location. This invention is restricted like the proxy server.

It is only possible to prevent or permit access of the terminal over a remote site.

In order to change the location which a specific terminal may access, this system is also static (static) at the point that it is necessary to reprogram the rule currently programmed in the database.

[0007]

The outline of invention

The principle which changes dynamically is created and enforced in this invention.

Therefore, redirection of the specifying data traffic for a specific user according to the activity of the database entry and the user, inhibition, or permission is enabled.

In the embodiment of this invention, if a user connects with a local network, user ID and a password will be transmitted to attestation and a fee collection server like the case where it is a publicly known system. User ID and a password are checked in the light of the information in an authentication database. A database also includes filtering according to individual corresponding to specific user ID, and redirection information. In the process of connection, a dial-up-networking server provides the IP address temporarily assigned to a user to attestation and a fee collection server. Subsequently, attestation and a fee collection server transmit all a user's momentary IP address, a specific user's filters, and redirection information to a redirection server. Since the IP address temporarily assigned to an end user uses it for connection with a network, it is returned to an end user.

[0008]

When it connects with a network, all the data packets transmitted and received among users will include the momentary IP address in the user's IP packet title. A redirection server by using the filter and redirection information from the attestation corresponding to the specific IP address, and a fee collection server, A packet is enabled to bypass a redirection server as it is, a request is prevented extensively, or a request is corrected according to redirection information.

[0009]

After a user ends connection with a network, a dial-up-networking server tells attestation and a fee collection server about that, and attestation and a fee collection server, A message is transmitted to a redirection server so that filtering and the redirection information corresponding to the momentary IP address of the user who ended connection may be removed. At this time, the dial-up networking can assign other users said IP address. In this case, attestation and a fee collection server retrieve a new user's filter and redirection information from a database, and a new user transmits them to a redirection server together with the same IP address to be used from now on. This new user's filter is not necessarily the same as that of the 1st user.

[0010]

DETAILED DESCRIPTION

In the following embodiment of this invention, a reference number common to expressing the same component part is used. If the feature of one embodiment is included in single system, such component part is shared and all the functions of a necessary embodiment can be achieved.

[0011]

Drawing 1 shows the typical Internet Service Provider (ISP) environment where it has an automatic data redirection system only for an intensive user. As a typical utilizing method of this system, a user uses the personal computer (PC) 100 linked to a network. A dial-up-networking server (102), attestation and the fee collection server 204, the database 206, and the redirection server 208 are used for this system.

[0012]

PC100 connects with the dial-up-networking server 102 first. Although this connection is usually made using a computer modem, the communication line of a Local Area Network (LAN) or others can also be used. The dial up network server 102 is a means for forming a communication line between a user's PC100 using a standard communications protocol. As a desirable embodiment, by using a point-to-point protocol (PPP), A physical circuit is established between PC100 and the dial-up-networking server 102, from the list of usable addresses, one IP address is chosen and dynamic assignment is carried out at PC100. However, it is also possible to carry out so that a different communications protocol from the above may be adopted and permanent residence assignment of the IP address may be carried out to PC100. Each of dial-up-networking servers 102, PPP, and dynamic IP address assignment is publicly known.

[0013]

The attestation and the fee collection server (attestation and a fee collection server are called hereafter) 204 which have Auto-Navi equipment attest user ID, and permit or refuse access to a network. Attestation and the fee collection server 204 are asked to the database 206, and user ID judges whether it is what justifies access to a network. If attestation and the fee collection server 204 judge that user ID is proper, Attestation and the fee collection server 204 receive the dial-up-networking server 102, Point so that an IP address may be assigned to PC100, and the Auto-Navi equipment of attestation and the fee collection server 204 receives the redirection server 208, (1) the filter in the database corresponding to this user ID and redirection information, and (2) -- transmit the IP address temporarily assigned for this session. An example of attestation and a fee collection server is indicated to US,5,845,070,B quoted in Description of this application for reference. The different attestation and fee collection server of a mode from this are also publicly known. However, these publicly known attestation and a fee collection server lack Auto-Navi equipment.

[0014]

The system described here operates based on the user ID given by computer. That is, a system "does not know" who the "user" who is facing to the keyboard of the computer which supplies user ID is. However, in many cases, the expression a "user" is used in order to express simply "the person which inputs into the computer which supplies specific user ID to a system" for detailed explanation.

[0015]

The database 206 is a relation database which memorizes system data. Drawing 2 shows one embodiment of database structure. In a desirable embodiment, a database includes the following field. That is, they are a user account number, the service (for example, e - mail, Telnet, FTP, WWW) with which each user was permitted or refused, and the place where each user was allowed access.

[0016]

A rule set (rule set) is adopted by a system, and is peculiar for every user ID or user group. A rule set specifies a user's element or conditions about a session. The rule set can contain a stage, a method, etc. of correcting a rule set during the kind of accessible or impossible service, an accessible or impossible place, the shelf-life of a rule set, the conditions from which a rule set is removed, and a session. Since removal from a system is ensured, the longest shelf-life of a rule set can also be set up beforehand.

[0017]

Logically, the redirection server 208 is located between a user's computer 100 and a network, and manages access of the user to a network. The redirection server 208 performs all the central tasks of a system. The redirection server 208 receives the information about the session materialized newly from attestation and the fee collection server 204. The Auto-Navi equipment of attestation and the fee collection server 204 asks a database the rule set which should be carried out a summary to each new session, and transmits a rule set and a quota IP address to the redirection server 208. The redirection server 208 receives an IP address and a rule set, performs a rule set about an IP address, and it is programmed to, perform the logic judging of the following accompanying for example. That is, it is checking a data packet, following a rule set, and preventing or permitting a packet, performing physical redirection of a data packet based on a rule set, and changing a rule set dynamically based on conditions. If the redirection server 208 receives the information about an end session from attestation and the fee collection server 204, the redirection server 208 will eliminate the information relevant to an unsolved rule set and session. the redirection server 208 is boiled every moment, and checks and eliminates a finished rule set again.

[0018]

In other embodiments, the redirection server 208 reports all or a part of session information to the database 206. This information is used for report creation or additional rule set creation.

[0019]

The feature outline of a system

In this embodiment, specific IP service, for example, WWW, FTP, and Telnet can be restricted or permitted to each specific user. For example, even when access to WWW is possible for a certain user, access to FTP or Telnet is impossible. Edit a user's database record and the nAuto-Navi equipment of attestation and the fee collection server 204 is received, By ordering a user's new rule set and this time IP address to transmit to the redirection server 208, a user's access can be changed dynamically.

[0020]

A user's access "can be locked" only at one place or 1 set of places. If the locked user is going to access other places, the redirection server 208 will redirect a user to a lack place. In this case, by acting as a substitute of a destination address, if the redirection server 208 is a case of WWW traffic, the redirection server 208 answers it to a user's request on a page including a redirection command.

[0021]

Based on time and other conditions, a user can also be periodically redirected to one place. For example, after redirecting to one place first regardless of the place which a user means, access to other places is allowed, but a user is automatically redirected to the first place every 10 minutes. The redirection server 208 performs such a rule set by setting up a rule set temporarily [initial] for redirecting all the traffic. If the place where the user was redirected is accessed, the redirection server 208 will replace a rule set with a user's standard rule set temporarily, or will remove a rule set from the redirection server 208 thoroughly. The redirection server 208 restores a rule set again after fixed time or variable time, for example, 10 minutes.

[0022]

The following steps are details of a typical user session.

- A user connects with the dial-up-networking server 102 via the computer 100.
- A user enters user ID and a password into the dial-up-networking server 10 using the computer 100 which sends information to attestation and the fee collection server 204.
- Attestation and the fee collection server 204 ask the database 206, and check the validity of user ID and a password.
- If a user's attestation is performed successfully, the dial-up-networking server 102 will complete a negotiation (negotiation), and will assign a user an IP address. In many cases, attestation and a fee collection server record connection on the database 206.
- The Auto-Navi equipment of attestation and the fee collection server 204, (It is contained in the database 206) A user's rule set and user (assigned by dial-up-networking server 102) IP address, A redirection server can be made to carry out the filter of the user IP packet by transmitting to the redirection server 208 in real time.
- The redirection server 208 programs a rule set and an IP address, and control a user's data according to a rule set (a filter, redirection, etc.).

[0023]

The logic of a typical user's rule set and accompanying and an example of operation are explained below.

The rule set for a specific user (namely, user UserID-2), Access is allowed by only website .us.com, Telnet service can be received, and logic is as follows if it says that access from all the servers in xyz.com is redirected to www.us.com.

[0024]

The database 206 includes the following record of several one about user UserID-2.

[Mathematical formula 1]

ID	UserID-2	
Password:	secret	
#####		
### Rule Sets ###		
#####		
#service	rule	expire
http	www.us.com	0
http	*.xyz.com=>www.us.com	0

[0025]

- A user starts a session and transmits user ID and a password (UserID-2 and confidential information) to the dial-up-networking server 102. If user ID and a password are right, attestation and the fee collection server 204 will accept formation of a session to the dial-up-networking server 102. The dial-up-networking server 102 assigns an IP address (for example, 10.0.0.1) to UserID-2, and transmits this IP address to attestation and the fee collection server 204.

[0026]

- The Auto-Navi equipment of attestation and the fee collection server 204 transmits a user's rule set and a user's IP address (10.0.0.1) to the redirection server 208.

[0027]

- The redirection server 208 programs a rule set and an IP address, according to this rule set, carries out the filter of a user's packet, and redirects it. In order to perform a rule set, the logic which the redirection server 208 adopts is as [

several 2] follows.

[Mathematical formula 2]

```
IF source IP-address = 10.0.0.1 AND
  ( ((request type = HTTP) AND (destination address = www.us.com) ) OR
    (request type = Telnet)
  ) THEN ok.
```

```
IF source IP-address = 10.0.0.1 AND
  ( (request type = HTTP) AND (destination address = *.xyz.com)
  ) THEN (redirect = www.us.com)
```

[0028]

The redirection server 208 monitors all the IP packets, and checks each packet in the light of a rule set. In this case, it is if IP address 10.0.0.1 (address assigned to user ID UserID-2) tends to transmit the packet containing HTTP data ().

That is, if it is going to connect with the machine port 80 in a xyz.com domain, traffic will be redirected to www.us.com. by the redirection server 208. Similarly, a packet is prevented by the redirection server 208 if a user is going to connect with the service of those other than HTTP in www.us.com, or Telnet.

If a user cuts logout or connection from a system, a redirection server will eliminate all residual rule sets.

[0029]

The logic of a typical user's rule set and accompanying and other examples of operation are explained below.
After making a user access website www.widgetsell.com first, if the rule set for a specific user (namely, user UserID-3) says that it makes other websites access, it is as follows. [of logic]
[0030]

The database 206 includes the following record of several three about user UserID-3.
[Mathematical formula 3]

ID	UserID-3	
Password:	top-secret	
#####		
### Rule Sets ###		
#####		
#service	rule	expire
http	*=> www.widgetsell.com	1x

- A user starts a session and transmits right user ID and a password (UserID-3 and extra sensitive information) to the dial-up-networking server 102. If user ID and a password are right, attestation and the fee collection server 204 will accept session formation to the dial-up-networking server 102. The dial-up-networking server 102 assigns an IP address (for example, 10.0.0.1) to the user ID 3, and transmits this IP address to attestation and the fee collection server 204.

[0031]

- The Auto-Navi equipment of attestation and the fee collection server 204 transmits IP address (10.0.0.1) of a user's rule set and a user to the redirection server 208.

[0032]

- The redirection server 208 programs a rule set and an IP address, according to this rule set, carries out the filter of a user's packet, and redirects it. In order to perform a rule set, the logic which the redirection server 208 adopts is as [several 4] follows.

[Mathematical formula 4]

```
IF source IP-address = 10.0.0.1 AND
  (request type = HTTP) THEN (redirect = www.widgetsell.com)

THEN SET NEW RULE
IF source IP-address = 10.0.0.1 AND
  (request type = HTTP) THEN ok.
```

[0033]

The redirection server 208 monitors all the IP packets, and checks each packet in the light of a rule set. In this case, it is if IP address 10.0.0.1 (address assigned to user ID UserID-3) tends to transmit the packet containing HTTP data (.). That is, if it is going to connect with the machine port 80, traffic will be redirected to www.widgetsell.com. by the redirection server 208. As a result, the redirection server 208 can eliminate a rule set and the user can use a web freely. If a user cuts logout or connection from a system, a redirection server will eliminate all residual rule sets.

[0034]

Based on many other factors, such as a type etc. of the place accessed, a user can also be periodically redirected to one place the time consumed as an embodiment of further others at the number of the places accessed, and one place, for example.

[0035]

Excess of predetermined time will intercept a user's communication. Attestation and the fee collection server 204 pursue a user's on-line time. If it is a prepaid member, it is easily manageable by attestation and the fee collection server 204.

[0036]

As an embodiment of further others, the rule set which the redirection server is using is correctable by using the signal from the Internet 110 side of the redirection server 208. Preferably, it is verifiable by using encryption and/or attestation whether the server or other computers by the side of the Internet 110 of the redirection server 208 are having correction of the rule set which is going to be corrected approved. this operative condition -- or [that an example / like / is answered to the questionnaire entries or the conditions in a specific website] -- or it is a case where a user must be redirected to this website until it is filled. In this example, a redirection server redirects a user to a specific website including questionnaire entries. If this website receives appropriate data in all the required columns, a website will permit excluding the redirection from the rule set of the user who has replied to questionnaire entries thoroughly to a question website to a redirection server. Of course, correction of the kind of others which the kind of correction which an external server can add to the rule set about a redirection server does not remain only in the abbreviation of a redirection rule, but are supported by redirection server which was mentioned above is also included.

[0037]

It can carry out so that, and service various type [, such as Telnet, FTP, and WWW,] may be controlled (inhibition, permission, redirection). [a person skilled in the art] This invention is programmed easily adapted for new service or network, and is not limited to publicly known service and network (for example, Internet).

[0038]

It cannot be overemphasized that it is applicable also to the network of non-IP base which performs other address schemes, such as IPX and a MAC Address, by one side. Although the operating environment which explained the desirable embodiment in full detail is a case of ISP which connects a user to the Internet, it is possible to apply, also when access of the user to a Local Area Network, a Wide Area Network, etc. must be controlled. So, neither environment nor a communications protocol is limited only to the matter examined so far.

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram showing typical Internet Service Provider environment.

[Drawing 2] It is a block diagram showing the embodiment of the Internet Service Provider environment where it has a concentration redirection system.

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第3588323号
(P3588323)

(45) 発行日 平成16年11月10日 (2004. 11. 10)

(24) 登録日 平成16年8月20日 (2004. 8. 20)

(51) Int. Cl. ⁷	F I		
H04 L 12/58	H04 L 12/58	1 O O F	
G06 F 13/00	G06 F 13/00	3 5 1 Z	
G06 F 15/00	G06 F 15/00	3 1 O A	
H04 L 12/56	H04 L 12/56	C	
	H04 L 12/56	2 O O Z	

請求項の数 29 (全 14 頁)

(21) 出願番号	特願2000-547748 (P2000-547748)	(73) 特許権者	500564987
(86) (22) 出願日	平成11年4月29日 (1999. 4. 29)		オーリック ウェブ システムズ
(65) 公表番号	特表2002-514802 (P2002-514802A)		アメリカ合衆国, カリフォルニア 9 1 1
(43) 公表日	平成14年5月21日 (2002. 5. 21)		O 7, パサデナ, イースト フットヒル
(86) 国際出願番号	PCT/US1999/009362		ブルバード 3 4 5 2, スイート 3 O
(87) 国際公開番号	W01999/057866		O
(87) 国際公開日	平成11年11月11日 (1999. 11. 11)	(74) 代理人	100077517
審査請求日	平成12年11月6日 (2000. 11. 6)		弁理士 石田 敬
(31) 優先権主張番号	60/084, 014	(74) 代理人	100092624
(32) 優先日	平成10年5月4日 (1998. 5. 4)		弁理士 鶴田 準一
(33) 優先権主張国	米国 (US)	(74) 代理人	100108383
(31) 優先権主張番号	09/295, 966		弁理士 下道 晶久
(32) 優先日	平成11年4月21日 (1999. 4. 21)	(74) 代理人	100082898
(33) 優先権主張国	米国 (US)		弁理士 西山 雅也

最終頁に続く

(54) 【発明の名称】 ユーザ専用のデータリダイレクションシステム、および、ユーザ専用のデータリダイレクション
を実行する方法

(57) 【特許請求の範囲】

【請求項 1】

複数のユーザ I D の各々を各ユーザ専用の規則セットに相関させる項目を含むデータベースと、
ユーザのコンピュータからユーザ I D を受け取るダイアルアップ・ネットワーク・サーバと、
前記ダイアルアップ・ネットワーク・サーバおよび公衆のネットワークに接続されている
リダイレクション・サーバと、
前記データベースと前記ダイアルアップ・ネットワーク・サーバと前記リダイレクション
・サーバとに接続されている認証および課金サーバとを含むユーザ専用の自動データリダ
イレクションシステムであって、
前記ダイアルアップ・ネットワーク・サーバは、前記ユーザのコンピュータの一つに対す
る第 1 のユーザ I D と前記第 1 のユーザ I D のための一時割当てネットワークアドレスと
を前記認証および課金サーバに伝送し、
前記認証および課金サーバは前記データベースにアクセスし、前記第 1 のユーザ I D と相
関する前記各ユーザ専用の規則セットと前記一時割当てネットワークアドレスとを前記リ
ダイレクション・サーバに伝送し、前記ユーザのコンピュータの一つから前記公衆のネッ
トワークに向けられたデータが、前記各ユーザ専用の規則セットに従って、前記リダイレ
クション・サーバにより処理されることを特徴とする、ユーザ専用の自動データリダイレ
クションシステム。

10

20

【請求項 2】

前記リダイレクション・サーバは、さらに、前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータに出入りする複数のデータに対する制御を行う請求項 1 に記載のシステム。

【請求項 3】

前記リダイレクション・サーバは、さらに、前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータに出入りするデータを阻止する請求項 1 に記載のシステム。

【請求項 4】

前記リダイレクション・サーバは、さらに、前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータに出入りするデータを許可する請求項 1 に記載のシステム。

10

【請求項 5】

前記リダイレクション・サーバは、さらに、前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータに出入りするデータをリダイレクトする請求項 1 に記載のシステム。

【請求項 6】

前記リダイレクション・サーバは、さらに、前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータからのデータを複数の宛先にリダイレクトする請求項 1 に記載のシステム。

【請求項 7】

前記複数のユーザ ID に関する前記データベース項目が共通の各ユーザ専用の規則セットに相関させられる請求項 1 に記載のシステム。

20

【請求項 8】

複数のユーザ ID の各々を各ユーザ専用の規則セットに相関させる項目を含むデータベースと、ユーザのコンピュータからユーザ ID を受け取るダイヤルアップ・ネットワーク・サーバと、前記ダイヤルアップ・ネットワーク・サーバおよび公衆のネットワークに接続されているリダイレクション・サーバと、前記データベースと前記ダイヤルアップ・ネットワーク・サーバと前記リダイレクション・サーバとに接続されている認証および課金サーバとを含むシステムにおいて、

前記ユーザのコンピュータの一つに対する第 1 のユーザ ID と前記第 1 のユーザ ID のための一時割当てネットワークアドレスとを、前記ダイヤルアップ・ネットワーク・サーバから前記認証および課金サーバに伝送する段階と、

30

前記第 1 のユーザ ID と相関する前記各ユーザ専用の規則セットと、前記一時割当てネットワークアドレスとを、前記認証および課金サーバから前記リダイレクション・サーバに伝送し、前記各ユーザ専用の規則セットに従って、前記ユーザのコンピュータの一つから前記公衆のネットワークに向けられたデータを処理する段階とを含むことを特徴とする、ユーザ専用の自動データリダイレクションを実行する方法。

【請求項 9】

前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータに出入りする複数のデータを制御する段階をさらに含む請求項 8 に記載の方法。

【請求項 10】

40

前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータに出入りするデータを阻止する段階をさらに含む請求項 8 に記載の方法。

【請求項 11】

前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータに出入りするデータを許可する段階をさらに含む請求項 8 に記載の方法。

【請求項 12】

前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータに出入りするデータをリダイレクトする段階をさらに含む請求項 8 に記載の方法。

【請求項 13】

前記各ユーザ専用の規則セットに応じて、前記ユーザのコンピュータからのデータを複数

50

の宛先にリダイレクトする段階をさらに含む請求項 8 に記載の方法。

【請求項 14】

前記複数のユーザ ID に関するデータベース項目を生成する段階をさらに含み、前記複数のユーザ ID は、さらに、共通の各ユーザ専用の規則セットに相関させられる請求項 8 に記載の方法。

【請求項 15】

一時割当てネットワークアドレスに相関しているユーザの規則セットを用いてプログラムされているリダイレクション・サーバを含むユーザ専用の自動データリダイレクションシステムであって、

前記規則セットは、前記ユーザと公衆のネットワークとの間で交換されるデータを制御するために使用される複数の関数の中の少なくとも一つの関数を含み、

前記リダイレクション・サーバは、前記一時割当てネットワークアドレスに相関している前記規則セットの少なくとも一部分の変更を可能にするように構成されていることを特徴とする、ユーザ専用の自動データリダイレクションシステム。

【請求項 16】

前記リダイレクション・サーバは、時間に応じて前記規則セットの少なくとも一部分の変更を可能にするように構成されている請求項 15 に記載のシステム。

【請求項 17】

前記リダイレクション・サーバは、ユーザに対して伝送されるかユーザから伝送されるデータに応じて、前記規則セットの少なくとも一部分の変更を可能にするように構成されている請求項 15 に記載のシステム。

【請求項 18】

前記リダイレクション・サーバは、ユーザがアクセスする一つまたは複数のロケーションに応じて、前記規則セットの少なくとも一部分の変更を可能にするように構成されている請求項 15 に記載のシステム。

【請求項 19】

前記リダイレクション・サーバは、時間、ユーザに伝送されるデータもしくはユーザから伝送されるデータ、または、ユーザがアクセスする一つまたは複数のロケーションの何らかの組合せに応じて、前記規則セットの少なくとも一部分の変更を可能にするように構成されている請求項 15 に記載のシステム。

【請求項 20】

前記リダイレクション・サーバは、時間に応じて前記規則の少なくとも一部分を削除または復元することを可能にするように構成されている請求項 15 に記載のシステム。

【請求項 21】

前記リダイレクション・サーバは、ユーザに伝送されるデータまたはユーザから伝送されるデータに応じて、前記規則セットの少なくとも一部分の削除または復元を可能にするように構成されている請求項 15 に記載のシステム。

【請求項 22】

前記リダイレクション・サーバは、ユーザがアクセスする一つまたは複数のロケーションに応じて、前記規則の少なくとも一部分の削除または復元を可能にするように構成されている請求項 15 に記載のシステム。

【請求項 23】

前記リダイレクション・サーバは、時間、ユーザに伝送されるデータもしくはユーザから伝送されるデータ、または、ユーザがアクセスする一つまたは複数のロケーションの何らかの組合せに応じて、前記規則の少なくとも一部分の削除または復元を可能にするように構成されている請求項 15 に記載のシステム。

【請求項 24】

前記リダイレクション・サーバは、前記一時割当てネットワークアドレスを使用するコンピュータに接続されているユーザ側と、コンピュータネットワークに接続されているネットワーク側とを有し、前記一時割当てネットワークアドレスを使用する前記コンピュータ

10

20

30

40

50

は前記リダイレクション・サーバを経由して前記コンピュータネットワークに接続されている請求項 15 に記載のシステム。

【請求項 25】

前記規則セットを変更するための前記リダイレクション・サーバに対する命令は、前記リダイレクション・サーバの前記ユーザ側と前記リダイレクション・サーバの前記ネットワーク側の一つ以上によって受け取られる請求項 24 に記載のシステム。

【請求項 26】

一時割当てネットワークアドレスに相関させられているユーザの規則セットを含むリダイレクション・サーバを含み、かつ、前記ユーザの規則セットは、前記ユーザと公衆のネットワークとの間で交換されるデータを制御するために使用される複数の関数の中の少なくとも一つの関数を含むシステムにおいて、

前記リダイレクション・サーバ内の前記一時割当てネットワークアドレスに前記ユーザの規則セットが相関させられているままである間に、前記ユーザの規則セットの少なくとも一部分を変更する段階を含むことを特徴とする、ユーザ専用のデータリダイレクションを実行する方法。

【請求項 27】

時間、ユーザに伝送されるデータまたはユーザから伝送されるデータ、および、ユーザがアクセスする一つまたは複数のロケーションの一つ以上に応じて、前記ユーザの規則セットの少なくとも一部分を変更する段階をさらに含む請求項 26 に記載の方法。

【請求項 28】

時間、ユーザに伝送されるデータまたはユーザから伝送されるデータ、および、ユーザがアクセスする一つまたは複数のロケーションの一つ以上に応じて、前記ユーザの規則セットの少なくとも一部分を削除または復元する段階をさらに含む請求項 26 に記載の方法。

【請求項 29】

前記リダイレクション・サーバは、前記一時割当てネットワークアドレスを使用するコンピュータに接続されているユーザ側と、コンピュータネットワークに接続されているネットワーク側とを有し、前記一時割当てネットワークアドレスを使用する前記コンピュータは前記リダイレクション・サーバを経由して前記コンピュータネットワークに接続されており、前記方法は、さらに、前記リダイレクション・サーバの前記ユーザ側と前記リダイレクション・サーバの前記ネットワーク側の一つ以上によって前記ユーザの規則セットの少なくとも一部分を変更するために、前記リダイレクション・サーバによる命令を受け取る段階を含む請求項 26 に記載の方法。

【発明の詳細な説明】

【0001】

発明の分野

本発明は、インターネット通信の分野に関し、より詳しくいえば、インターネットのトラフィックを動的にリダイレクト (redirect) およびフィルタ (filter) することに使用するためのデータベースに関する。

【0002】

発明の背景

図 1 に示すような従来のシステムでは、インターネットのユーザがインターネットサービスプロバイダ (ISP) との接続を樹立するとき、ユーザは最初に自分のコンピュータ 100 とダイアルアップ・ネットワーク・サーバ (ダイアル呼出し・ネットワーク・サーバともよばれる) 102 との間に物理的接続を確立して、そのダイアルアップ・ネットワーク・サーバ 102 に自分のユーザ ID とパスワードとを提供する。その次に、ダイアルアップ・ネットワーク・サーバは、ユーザ ID とパスワードとを、そのユーザによる使用のための一時的なインターネットプロトコル (IP) アドレスと共に、ISP の認証および課金サーバ 104 に送る。IP 通信プロトコルの詳細な説明は、“Internet working with TCP/IP, 3rd ed., Douglas Comer, Prentice Hall, 1995” に記載されており、この内容全体が本明細書

10

20

30

40

50

に引例として組み入れてある。認証および課金サーバは、データベース106を使用してユーザIDとパスワードとを検査するときに、ダイアルアップ・ネットワーク・サーバによってユーザに割り当てられている一時IPアドレスをそのユーザが使用することを可能にするために、認証メッセージをダイアルアップ・ネットワーク・サーバ102に送り、その次に接続と割当てIPアドレスとを記録する。このセッション中は、ユーザがゲートウェイ108を経由してインターネット110に対して要求を行うときにはいつでも、このエンドユーザは一時割当てIPアドレスによって識別されることになる。

【0003】

インターネット・トラフィックのリダイレクションは、ワールドワイドウェブ（WWW）トラフィック（さらに明確に述べると、HTTP（ハイパーテキスト転送プロトコル）を使用するトラフィック）に関して行われることが最も多い。しかし、リダイレクションはWWWトラフィックに限定されておらず、この着想は全てのIPサービスに有効である。どのようにリダイレクションが行われるかを示すために、WWWページ（典型的には、html（ハイパーテキストマークアップ言語）ファイル）を求めるユーザの要求を何らかの他のWWWページにリダイレクトする次の事例を考察することにする。まず最初に、ユーザは、URL（ユニバーサル・リソース・ロケータ）をタイプ入力するかURLリンクをクリックすることによって、WWWブラウザ（典型的には、ユーザのPC上で動作するソフトウェア）に、リモートWWWサーバ上のページにアクセスするように命令する。通信プロトコルと、サーバのロケーション（典型的には、インターネットドメイン名またはIPアドレス）と、リモートサーバ上の当該ページのロケーションとに関する情報をURLが提供するという点に留意されたい。その次に、ブラウザは、サーバに要求を送り、該当ページを要求する。このユーザの要求にตอบสนองして、ウェブサーバは、要求されたページをブラウザに送る。しかし、このページは、そのブラウザに何らかの他のWWWページを要求するように命令するhtmlコードを含み、したがって、ユーザのリダイレクションが始まる。その次に、ブラウザは、最初のページのhtmlコードに含まれたURLにしたがって、リダイレクトされたWWWページを要求する。あるいは、Javaアプレット等のようなプログラムをブラウザに実行するように命令し、このプログラムがブラウザをリダイレクトするようにページをコード化することによっても、リダイレクションが行われることが可能である。現行のリダイレクション技術の欠点の一つは、リダイレクションの制御がリモート側すなわちWWWサーバ側であり、ローカル側すなわちユーザ側ではないということである。すなわち、リダイレクションがリモートサーバによって行われ、ユーザのローカルゲートウェイによっては行われない。

【0004】

ここ数年の間に、ファイアウォール装置または他のパケットフィルタリング装置を使用することによって、インターネットプロトコル（IP）層におけるパケットのフィルタリングを行うことが可能となっている。パケットのフィルタリングは、セキュリティの目的から、私設ネットワークの中に入ってくるパケットをフィルタするために使用されることが最も多いが、適正にプログラムされる場合には、ユーザから特定の宛先に送られる出力パケットをフィルタすることも可能である。パケットフィルタリングは、IPパケット内に含まれるIPサービスのタイプを識別し、これの識別に基づいてフィルタリングを行うことが可能である。例えば、パケットフィルタは、パケットがFTP（ファイル転送プロトコル）データ、WWWデータ、または、Telnetセッションデータを含むかどうかを判定することが可能である。このサービス識別は、各々のIPパケットヘッダ内に含まれている終端ポート番号を識別することによって実現される。ポート番号は、装置間の相互運用性を実現するために、業界の標準規格に従っている。パケットフィルタリング装置は、ソースおよび／または宛先情報と各IPパケット内で伝送されるサービスのタイプとに基づいてネットワーク管理者がパケットをフィルタすることを可能にする。リダイレクション技術とは違って、パケットフィルタリング技術は、ネットワーク接続のローカル側での制御を可能にし、典型的にはネットワーク管理者による制御を可能にする。しかし、パケットフィルタリングは、静的であるために、非常に制限されている。パケットフィルタ

リング規則がいったんファイアウォール装置または他のパケットフィルタリング装置にプログラムされると、こうした装置を手作業で再プログラムすることによってしか、設定したパケットフィルタリング規則を変更できない。

【0005】

パケットフィルタリング装置は、プロキシサーバシステムと共に使用されることが多く、このプロキシサーバシステムはインターネットに対するアクセスの制御を実現し、WWWに対するアクセスを制御するために使用されることが最も多い。典型的な構成では、ファイアウォール装置または他のパケットフィルタリング装置は、プロキシサーバからのパケットを除いて、インターネットに対するローカルネットワークからのWWW要求の全てをフィルタする。すなわち、パケットフィルタまたはファイアウォールは、ポート80（標準WWWポート番号）上のリモートサーバに接続されるようになっている、ローカルネットワーク内から送出されるトラフィック全てを阻止する。しかし、このパケットフィルタまたはファイアウォールは、プロキシサーバ（proxy server）に対して送受されるこうしたトラフィックは許容する。典型的には、プロキシサーバは、阻止されなければならない1組の宛先を伴ってプログラムされており、阻止されたアドレスに仕向けられたパケットは転送されない。プロキシサーバがパケットを受け取るときには、承認を得るために宛先がデータベースと対照して検査される。その宛先が認可されると、プロキシサーバは単にそのパケットをローカルユーザとファイアウォールの外側のリモートサーバとの間で転送する。しかし、プロキシサーバは、リモートデータベースに対する特定のシステム端末のアクセスを阻止または許可することに限定されている。

【0006】

最近のシステムが米国特許第5,696,898号に開示されている。この特許は、ファイアウォールの内側の特定のIPアドレスが特定の公開データベースまたは（そうでない場合には）制御不可なデータベース（すなわち、WWW/インターネット）からの情報にアクセスすることをネットワーク管理者が制限することを可能にする、プロキシサーバに類似したシステムを開示している。この開示内容によれば、このシステムは、特定の端末または端末グループが特定のロケーションにアクセスすることをネットワーク管理者が制限することを可能にするリレーショナルデータベースを有する。この発明は、プロキシサーバと同様に制限されており、リモートサイトに対する端末のアクセスを阻止または許可することだけが可能であるにすぎない。さらに、特定の端末がアクセスしてよいロケーションを変更するためには、データベースの中にプログラムされている規則を再プログラムする必要があるという点で、このシステムも静的（static）である。

【0007】

発明の概要

本発明はダイナミックに変化する法則を創造し、実施することにより、データベース・エントリおよびユーザの活動に応じた、特定ユーザのための特定データ・トラフィックのリダイレクション、阻止または許可を可能にする。本発明の実施例では、ユーザがローカル・ネットワークと接続すると、公知システムの場合と同様に、ユーザIDおよびパスワードが認証および課金サーバに送信される。ユーザIDおよびパスワードが、認証データベース中の情報に照らしてチェックされる。データベースは特定ユーザIDに対応する個人別のフィルタリングおよびリダイレクション情報をも含む。接続の過程において、ダイヤルアップ・ネットワーク・サーバは認証および課金サーバに対し、ユーザに一時的に割り当てられるIPアドレスを提供する。次いで、認証および課金サーバはリダイレクション・サーバに、ユーザの一時IPアドレス、および特定ユーザのフィルタおよびリダイレクション情報のすべてを送信する。エンド・ユーザに一時的に割り当てられるIPアドレスは、ネットワークとの接続に使用するため、エンド・ユーザに返送される。

【0008】

ネットワークに接続すると、ユーザとの間で送受信されるすべてのデータ・パケットは、そのユーザのIPパケット見出し中の一時IPアドレスを含むことになる。リダイレクション・サーバは、その特定IPアドレスに対応する認証および課金サーバからのフィルタ

およびリダイレクション情報を利用することによって、パケットがそのままリダイレクション・サーバを素通りすることを可能にするか、リクエストを全面的に阻止するか、または、リダイレクション情報に従ってリクエストを修正する。

【0009】

ユーザがネットワークとの接続を終了すると、ダイヤルアップ・ネットワーク・サーバはそのことを認証および課金サーバに知らせ、認証および課金サーバは、接続を終了したユーザの一時IPアドレスに対応するフィルタリングおよびリダイレクション情報を取り除くようリダイレクション・サーバにメッセージを送信する。この時点で、ダイヤルアップ・ネットワークは前記IPアドレスを他のユーザに割り当てることができる。この場合、認証および課金サーバはデータベースから新しいユーザのフィルタおよびリダイレクション情報を検索し、新しいユーザがこれから使用する同じIPアドレスと一緒に、リダイレクション・サーバに送信する。この新しいユーザのフィルタは第1のユーザのフィルタと同じとは限らない。

【0010】

発明の詳細な説明

本発明の下記実施例において、同じ構成部分を表すのに共通の参照番号を使用する。一実施例の特徴を単一システムに組み込めば、これらの構成部分が共用されて、所要実施例のすべての機能を果たすことができる。

【0011】

図1は集中的なユーザ専用の自動データリダイレクションシステムを有する典型的なインターネットサービスプロバイダ（ISP）環境を示す。このシステムの典型的な利用方法として、ユーザはネットワークと接続するパソコン（PC）100を使用する。このシステムは、ダイヤルアップ・ネットワーク・サーバ（102）、認証および課金サーバ204、データベース206およびリダイレクション・サーバ208を使用する。

【0012】

PC100はまずダイヤルアップ・ネットワーク・サーバ102と接続する。この接続はコンピュータ・モデムを利用して行なわれるのが普通であるが、ローカルエリアネットワーク（LAN）またはその他の通信回線を利用することもできる。ダイヤルアップ・ネットワーク・サーバ102は、標準通信プロトコルを利用してユーザのPC100との間に通信回線を成立させるための手段である。好ましい実施態様としては、2地点間プロトコル（PPP）を利用することによって、PC100とダイヤルアップ・ネットワーク・サーバ102との間に物理的回線を確立し、使用可能なアドレスのリストから、一つのIPアドレスを選んでPC100にダイナミック割り当てする。但し、上記とは異なる通信プロトコルを採用し、PC100に対してIPアドレスを常駐割り当てするように実施することも可能である。なお、ダイヤルアップ・ネットワーク・サーバ102、PPPおよびダイナミックIPアドレス割り当てはいずれも公知である。

【0013】

Auto-Navi装置を有する認証および課金サーバ（以下、認証および課金サーバと呼称する）204は、ユーザIDを認証し、ネットワークへのアクセスを許可または拒絶する。認証および課金サーバ204はデータベース206に問い合わせ、ユーザIDがネットワークへのアクセスを正当化するものかどうかを判定する。もし、認証および課金サーバ204がユーザIDを適正と判定すると、認証および課金サーバ204はダイヤルアップ・ネットワーク・サーバ102に対して、PC100にIPアドレスを割り当てよう指示し、認証および課金サーバ204のAuto-Navi装置がリダイレクション・サーバ208に対して、（1）このユーザIDに対応するデータベース中のフィルタおよびリダイレクション情報と、（2）このセッションのため一時的に割り当てられるIPアドレスとを送信する。認証および課金サーバの一例は、参考のため本願明細書中に引用した米国特許第5,845,070号に記載されている。これとは異なる態様の認証および課金サーバも公知である。但し、これらの公知認証および課金サーバにはAuto-Navi装置が欠如している。

10

20

30

40

50

【0014】

ここに述べるシステムは、コンピュータによって与えられるユーザIDに基づいて動作する。すなわち、システムは、ユーザIDを供給するコンピュータのキーボードに向かって「ユーザ」が誰であるかを「知らない」。但し、詳細な説明のため、「システムに特定ユーザIDを供給するコンピュータに入力する人物」を簡単に表現するため、多くの場合、「ユーザ」という表現を使用する。

【0015】

データベース206はシステム・データを記憶する関連データベースである。図2はデータベース構造の一実施例を示す。好ましい実施態様では、データベースが下記のフィールドを含む。すなわち、ユーザ課金番号、各ユーザが許可または拒絶されたサービス（例えば、eメール、テルネット、FTP、WWW）、および、各ユーザがアクセスを許された場所である。

【0016】

規則セット（rule set）がシステムによって採用され、各ユーザIDまたは各ユーザ・グループ毎に固有である。規則セットはユーザのセッションに関する要素または条件を特定する。規則セットは、アクセス可能な、または不可能なサービスの種類、アクセス可能な、または不可能な場所、規則セットの有効期間、規則セットが除去される条件、セッション中に規則セットを修正する時期および方法などを含むことができる。システムからの除去を確実にするため、規則セットの最長有効期間を予め設定することもできる。

【0017】

リダイレクション・サーバ208は、論理的にはユーザのコンピュータ100とネットワークとの間に位置し、ネットワークへのユーザのアクセスを管理する。リダイレクション・サーバ208はシステムのすべての中央タスクを行なう。リダイレクション・サーバ208は、新しく成立したセッションに関する情報を認証および課金サーバ204から受信する。認証および課金サーバ204のAuto-Navi装置は、それぞれの新しいセッションに摘要すべき規則セットをデータベースに問い合わせ、リダイレクション・サーバ208に規則セットおよび割り当てIPアドレスを送信する。リダイレクション・サーバ208はIPアドレスおよび規則セットを受信し、IPアドレスに関して規則セットを実行すると共に、例えば、下記のような付随の論理判定を行うようにプログラムされる。すなわち、データ・パケットをチェックして、規則セットに従ってパケットを阻止または許可すること、規則セットに基づいてデータ・パケットの物理的リダイレクションを行うこと、および、条件に基づいて規則セットをダイナミックに変更することである。リダイレクション・サーバ208が認証および課金サーバ204から、終了セッションに関する情報を受信すると、リダイレクション・サーバ208は未解決の規則セットおよびセッションに関連する情報を消去する。リダイレクション・サーバ208はまた、時々刻々に用済みの規則セットをチェックし、消去する。

【0018】

他の実施例では、リダイレクション・サーバ208がセッション情報のすべてまたは一部をデータベース206に報告する。この情報は報告作成または追加規則セット作成に利用される。

【0019】

システムの特徴概説

この実施例では、それぞれの特定ユーザに対して、特定IPサービス、例えば、WWW、FTPおよびテルネットを制限したり、許可したりすることができる。例えば、或るユーザはWWWへのアクセスは可能でも、FTPまたはテルネットへのアクセスは不可能である。ユーザのデータベース記録を編集し、認証および課金サーバ204のAuto-Navi装置に対して、ユーザの新しい規則セットおよび現時点IPアドレスをリダイレクション・サーバ208へ転送するよう命令することによって、ユーザのアクセスをダイナミックに変更することができる。

【0020】

ユーザのアクセスを一つの場所だけに、または1組の場所だけに「ロック」することができる。ロックされたユーザが他の場所にアクセスしようとする、リダイレクション・サーバ208がユーザを欠如場所へリダイレクトする。この場合、リダイレクション・サーバ208は行き先アドレスの代理として作用するか、または、WWWトラフィックの場合なら、リダイレクション・サーバ208はユーザのリクエストに対して、リダイレクション命令を含むページで回答する。

【0021】

時間その他の条件に基づいて、ユーザを一つの場所へ周期的にリダイレクトすることもできる。例えば、ユーザが意図する場所に関係なく、先ず一つの場所へリダイレクトしてから、他の場所へのアクセスを許すが、10分ごとに自動的にユーザを最初の場所へリダイレクトする。リダイレクション・サーバ208は、すべてのトラフィックをリダイレクトするための初期一時規則セットを設定することによって、このような規則セットを行う。ユーザがリダイレクトされた場所にアクセスすると、リダイレクション・サーバ208は一時規則セットをユーザの標準規則セットに代えるか、またはリダイレクション・サーバ208から規則セットを完全に除去する。一定時間または可変時間、例えば10分後、リダイレクション・サーバ208は規則セットを再び復旧する。

【0022】

以下のステップは典型的なユーザ・セッションの詳細である。

・コンピュータ100を介してユーザがダイヤルアップ・ネットワーク・サーバ102と接続する。

・認証および課金サーバ204に情報を送るコンピュータ100を利用して、ユーザがユーザIDおよびパスワードをダイヤルアップ・ネットワーク・サーバ102に入力する。

・認証および課金サーバ204がデータベース206に問い合わせ、ユーザIDおよびパスワードの有効性をチェックする。

・ユーザの認証が成功裡に行われると、ダイヤルアップ・ネットワーク・サーバ102がネゴシエーション (negotiation) を完了し、ユーザにIPアドレスを割り当てる。多くの場合、認証および課金サーバはデータベース206に接続を記録する。

・認証および課金サーバ204のAuto-Nav装置は、(データベース206に含まれている) ユーザの規則セットと、(ダイヤルアップ・ネットワーク・サーバ102によって割り当てられた) ユーザIPアドレスとを、リアルタイムでリダイレクション・サーバ208に送信することにより、リダイレクション・サーバがユーザIPパケットをフィルタできるようにする。

・リダイレクション・サーバ208は規則セットおよびIPアドレスをプログラムして、規則セットに応じてユーザのデータを制御 (フィルタ、リダイレクトなど) する。

【0023】

典型的なユーザの規則セットおよび付随の論理および動作の例を以下に説明する。

特定ユーザ (すなわち、ユーザUser ID-2) のための規則セットが、ウェブ・サイト、us.comにのみアクセスを許され、テルネット・サービスを受けることができ、xyz.comにおけるすべてのサーバからのアクセスがwww.us.comへリダイレクトされるというものであれば、論理は下記のようなになる。

【0024】

データベース206はユーザUser ID-2に関して下記の数1の記録を含む。

【数1】

10

20

30

40

ID UserID-2
Password: secret

Rule Sets ###
#####

#service	rule	expire
http	www.us.com	0
http	*.xyz.com=>www.us.com	0

10

【0025】

・ユーザはセッションを開始し、ダイヤルアップ・ネットワーク・サーバ102にユーザIDおよびパスワード（UserID-2および秘密情報）を送信する。ユーザIDもパスワードも正しければ、認証および課金サーバ204はダイヤルアップ・ネットワーク・サーバ102に対して、セッションの成立を認める。ダイヤルアップ・ネットワーク・サーバ102はUserID-2にIPアドレス（例えば、10.0.0.1）を割り当て、このIPアドレスを認証および課金サーバ204に送信する。

【0026】

・認証および課金サーバ204のAuto-Navi装置は、ユーザの規則セットとユーザのIPアドレス（10.0.0.1）をリダイレクション・サーバ208に送信する。

20

【0027】

・リダイレクション・サーバ208は規則セットおよびIPアドレスをプログラムして、ユーザのパケットをこの規則セットに従ってフィルタし、リダイレクトする。規則セットを実行するためにリダイレクション・サーバ208が採用する論理は下記の数2の通りである。

【数2】

IF source IP-address = 10.0.0.1 AND

 (((request type = HTTP) AND (destination address = www.us.com)) OR
 (request type = Telnet)
) THEN ok.

30

IF source IP-address = 10.0.0.1 AND

 ((request type = HTTP) AND (destination address = *.xyz.com)
) THEN (redirect = www.us.com)

【0028】

リダイレクション・サーバ208はすべてのIPパケットをモニタし、規則セットに照らしてそれぞれのパケットをチェックする。この場合、もしIPアドレス10.0.0.1（ユーザID UserID-2に割り当てられたアドレス）がHTTPデータを含むパケットを送信しようとする（すなわち、xyz.comドメイン内のマシン・ポート80に接続しようとする）、トラフィックはリダイレクション・サーバ208によってwww.us.comへリダイレクトされる。同様に、もしユーザがwww.us.comにおけるHTTP以外のサービスまたはテルネットに接続しようとする、パケットはリダイレクション・サーバ208によって阻止される。ユーザがシステムからログアウトまたは接続を切ると、リダイレクション・サーバは残余の規則セットをすべて消去する。

40

【0029】

50

典型的なユーザの規則セットおよび付随の論理および動作の他の例を以下に説明する。
 特定ユーザ（すなわち、ユーザU s e r I D - 3）のための規則セットが、ユーザを先ず
 ウェブ・サイトw w w . w i d g e t s e l l . c o m にアクセスさせてから、他のウ
 ェブ・サイトにアクセスさせるというものであれば、論理は下記のようになる。

【0030】

データベース206はユーザU s e r I D - 3に関して下記の数3の記録を含む。

【数3】

ID	UserID-3
Password:	top-secret
#####	
### Rule Sets ###	
#####	
#service	rule
http	*=>www.widgetsell.com
expire	1x

10

・ユーザがセッションを開始し、正しいユーザIDおよびパスワード（U s e r I D - 3
 および極秘情報）をダイヤルアップ・ネットワーク・サーバ102に送信する。ユーザI
 Dもパスワードも正しければ、認証および課金サーバ204がダイヤルアップ・ネットワ
 ーク・サーバ102に対して、セッション成立を認める。ダイヤルアップ・ネットワ
 ーク・サーバ102はユーザID3にIPアドレス（例えば、10.0.0.1）を割り当て
 、このIPアドレスを認証および課金サーバ204に送信する。

20

【0031】

・認証および課金サーバ204のA u t o - N a v i 装置は、ユーザの規則セットとユー
 ザのIPアドレス（10.0.0.1）をリダイレクション・サーバ208に送信する
 。

【0032】

・リダイレクション・サーバ208は規則セットおよびIPアドレスをプログラムして、
 ユーザのパケットをこの規則セットに従ってフィルタし、リダイレクトする。規則セット
 を実行するためにリダイレクション・サーバ208が採用する論理は下記の数4の通りで
 ある。

30

【数4】

```

IF source IP-address = 10.0.0.1 AND
  (request type = HTTP) THEN (redirect = www.widgetsell.com)

THEN SET NEW RULE
IF source IP-address = 10.0.0.1 AND
  (request type = HTTP) THEN ok.
  
```

40

【0033】

リダイレクション・サーバ208はすべてのIPパケットをモニタし、規則セットに照ら
 してそれぞれのパケットをチェックする。この場合、もしIPアドレス10.0.0.1
 （ユーザID U s e r I D - 3に割り当てられたアドレス）がHTTPデータを含むパ
 ケットを送信しようとする（すなわち、マシン・ポート80に接続しようとする）と、
 トラフィックはリダイレクション・サーバ208によってw w w . w i d g e t s e l l
 . c o m . へリダイレクトされる。この結果、リダイレクション・サーバ208は規則セ
 ャットを消去し、ユーザは自由にウェブを利用することができる。

ユーザがシステムからログアウトまたは接続を切ると、リダイレクション・サーバは残余

50

の規則セットをすべて消去する。

【0034】

さらに他の実施態様として、例えば、アクセスされる場所の数、一つの場所で消費される時間、アクセスされる場所のタイプなどのような他の多くの要因に基づいて、ユーザを周期的に一つの場所へリダイレクトすることもできる。

【0035】

所定時間を超過すると、ユーザの通信は遮断される。認証および課金サーバ204はユーザのオンライン時間を追跡する。プリペイド加入者ならば、認証および課金サーバ204によって容易に管理することができる。

【0036】

さらに他の実施態様として、リダイレクション・サーバ208のインターネット110側からの信号を利用することによって、リダイレクション・サーバが使用している規則セットを修正することができる。好ましくは、暗号化および／または認証を利用することによって、リダイレクション・サーバ208のインターネット110側のサーバまたは他のコンピュータが、修正されようとしている規則セットの修正を是認されているかどうかを検証することができる。この実施態様の一例は、特定のウェブ・サイトにおける質問事項または条件が回答されるかまたは満たされるまで、ユーザをこのウェブ・サイトにリダイレクトしなければならない場合である。この例では、リダイレクション・サーバは、質問事項を含む特定ウェブ・サイトにユーザをリダイレクトする。このウェブ・サイトがすべての必要欄に然るべきデータを受信すると、ウェブ・サイトは、質問事項に完全に回答できたユーザの規則セットから、質問ウェブ・サイトへのリダイレクションを省くことを、リダイレクション・サーバに許可する。勿論、外部サーバがリダイレクション・サーバに関する規則セットに加えることができる修正の種類はリダイレクション・ルールの省略だけにとどまらず、前述したようなリダイレクション・サーバによって支持されるその他の種類の修正も含まれる。

【0037】

当業者には明白なように、テルネット、FTP、WWWなど、多様なタイプのサービスを制御（阻止、許可、リダイレクション）するように実施することができる。本発明は新しいサービスまたはネットワークに適応できるように容易にプログラムされ、公知のサービスおよびネットワーク（例えば、インターネット）に限定されるものではない。

【0038】

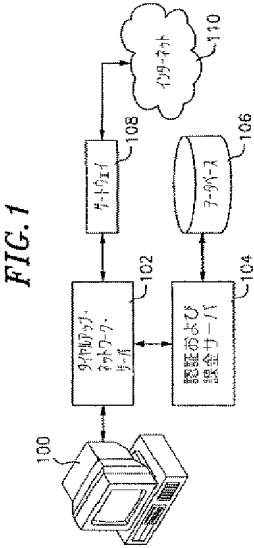
また一方で、IPX、MACアドレスなどのような他のアドレス・スキームを実行する非IPベースのネットワークにも応用できることはいうまでもない。好ましい実施例について詳述した使用環境はユーザをインターネットに接続するISPの場合であるが、ローカルエリアネットワーク、ワイドエリアネットワークなどへのユーザのアクセスを制御しなければならない場合にも応用することが可能である。それゆえに、環境および通信プロトコルのいずれも、これまで検討してきた事項のみに限定されない。

【図面の簡単な説明】

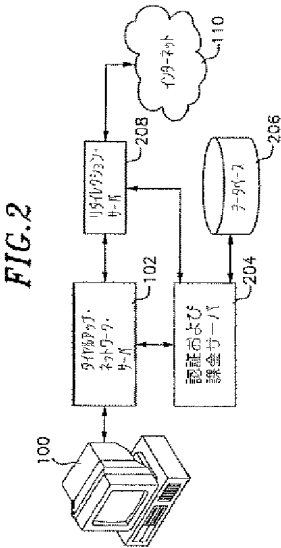
【図1】 典型的なインターネット・サービス・プロバイダ環境を示すブロック図である。

【図2】 集中リダイレクション・システムを有するインターネット・サービス・プロバイダ環境の実施例を示すブロック図である。

【図 1】



【図 2】



フロントページの続き

(74)代理人 100081330

弁理士 樋口 外治

(72)発明者 イクドメ, コウイチロウ

アメリカ合衆国, カリフォルニア 91007, アーカディア, ボランテ 857

(72)発明者 ユン, ムーン タイ

アメリカ合衆国, カリフォルニア 91801, アルハンブラ, ノース ファースト ストリート
819, アpartment ディー

審査官 田中 庸介

(56)参考文献 特開平10-070576 (JP, A)

国際公開第98/026548 (WO, A1)

(58)調査した分野(Int.Cl.⁷, DB名)

H04L 12/00-12/26

12/50-12/66

G06F 13/00, 351-357

G06F 15/00-15/00, 390